ExtremeXOS ScreenPlay User Guide

Copyright © 2001—2013 Extreme Networks

AccessAdapt, Alpine, Altitude, BlackDiamond, Direct Attach, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Ridgeline, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, XNV, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrive logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is the property of InMon Corporation.

iBooks is property of Apple, Inc.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

Published: October 2013

Part number: 100400-00_Rev_02

Table of Contents

Chapter 1: Overview 4

Chapter 2: Setting Up ScreenPlay 5

HTTP and HTTPS Setup 5
Client Setup 6
Launching ScreenPlay 6

Chapter 3: ScreenPlay Dashboard 7

ScreenPlay Common Functions 8

Chapter 4: Configuration 14

Configuration--Ports 14
Configuration--VLANs 18
Configuration--Stacking 21
Configuration--SNMP 22
Configuration--Dynamic ACLs 24

Chapter 5: Statistics and Monitoring 27

Statistics and Monitoring--Event Log 27
Statistics and Monitoring--Ports 28
Statistics and Monitoring--QoS 30

Chapter 6: Administration 32

Administration--User Accounts 32
Administration--User Sessions 35
Administration--CLI Shell 36

Chapter 7: Help 38

1 Overview

ScreenPlay is a web-based device management tool for all ExtremeXOS-based devices running software version 12.0 or higher. ScreenPlay is launched as a web page on the device. The ScreenPlay client, loaded onto the web browser, uses SOAP over HTTP to communicate with the device using XML APIs. ScreenPlay provides a graphical user interface for the more commonly used CLI commands, with focus on the statistics and monitoring commands.

Note

The screens shown in this chapter were captured from a variety of Extreme Networks switches. In some cases the information displayed on the screen varies somewhat depending on the switch being used.

2 Setting Up ScreenPlay

HTTP and HTTPS Setup
Client Setup
Launching ScreenPlay

This section describes the setup process required to use ScreenPlay with the switch and includes the following topics:

- HTTP and HTTPS Setup
- Client Setup
- Launching ScreenPlay

HTTP and HTTPS Setup

Before you can launch ScreenPlay, you must enable the web server on the switch. You can use either HTTP or HTTPS to access ScreenPlay.

Note
You must assign an IP address to a VLAN for management access to the switch. For more information, see the chapter Configuring Management Access.

1 To enable HTTP web access, enter the following command:

```
SummitX450a-48t.1 # enable web http
```

The switch is now ready for web access using HTTP at the URL `http://<switch_ip>`.

2 To enable HTTPS web access, you must first check to see if the SSL module is installed. Enter the following command:

```
BD-8806.1 # show ssl
```

If the following displays, the SSL module is not installed:

```
SSL Module: Not Installed BD-8806.2 #
```

The SSL module must be installed to enable HTTPS web access. (Refer to the *ExtremeXOS Concepts Guide* Secure Socket Layer in the Security chapter and Guidelines for Activating SSL in the Software Upgrade and Boot Options appendix.)

3 After the SSL module is installed, create a certificate by entering the following command:

```
BD-8806.2 # configure ssl certificate privkeylen 1024 country us
organization extreme common-name name1
```

4 To enable HTTPS web access, enter the following command:

```
SummitX450a-48t.1 # enable web https
```

The switch is now ready for web access using HTTPS at the URL `https://<switch_ip>`.

Client Setup

You need a standard web browser such as Mozilla Firefox® (version 1.0 or greater) or Internet Explorer® (version 6.0 or greater) with the Adobe Flash® Player 9 plug-in installed.

Note
ScreenPlay supports up to six concurrent sessions.

Launching ScreenPlay

1 To launch ScreenPlay, enter the URL of the switch in the address window of your browser.

When ScreenPlay launches, the authentication screen displays, as shown in the figure below.

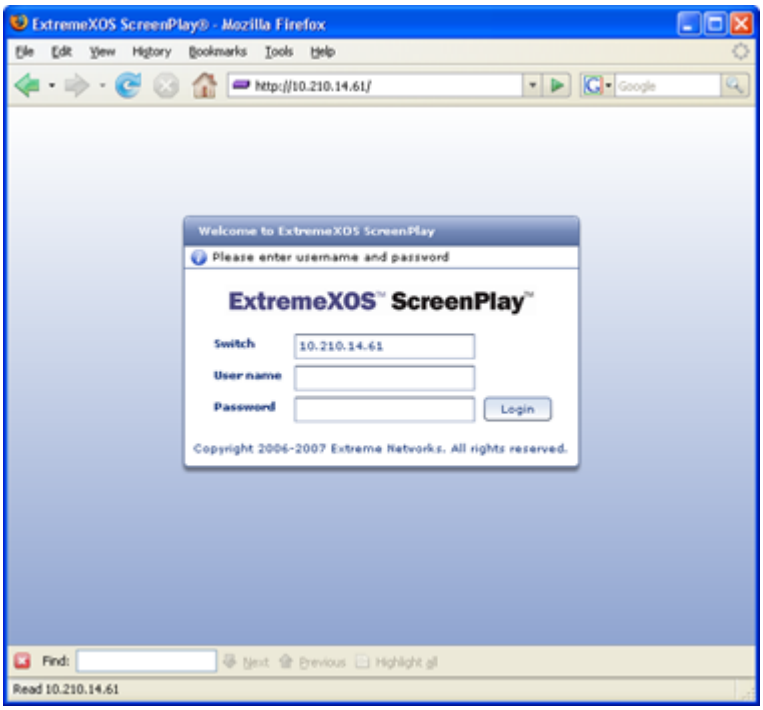


Figure 1: Login Window

2 The ScreenPlay login window displays the switch IP address. You must enter a user name and password for access. The user name and password used are the same that you use to access the CLI from a Telnet or SSH session.

3 ScreenPlay Dashboard

ScreenPlay Common Functions

Next, the ScreenPlay Dashboard appears. The dashboard is the home screen, or opening screen, of ScreenPlay. This screen provides you with a one-glance-snapshot of switch status, inventory, and management details. The main dashboard is divided into three information panes that are shown in the figure below and described in the subsequent table.

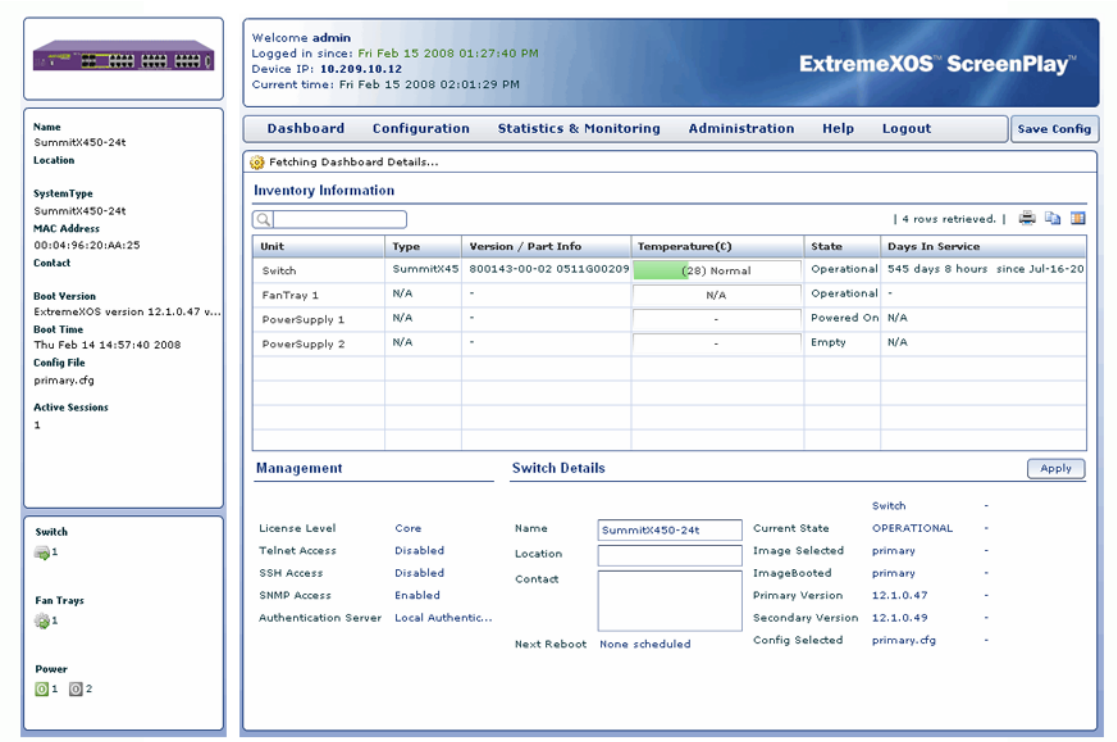


Figure 2: Dashboard Details

Table 1: Dashboard Details

Name	Description and Function
Switch Summary (left-hand pane)	Contains summary information about the switch, including: • The switch name, location, system type, MAC address, and boot version. • Hardware information, such as the number of slots, fan trays, and power modules in the switch as well as the status of those elements. Click items in this pane to see more detailed information about the items. For example, clicking a slot provides you with such slot information as its state, serial number, and temperature. Refer to Figure 3: Unit Information Screen on page 11. This pane remains consistent across all views.
Header	Displays information about the current session including: • The logged in user; the date and time when the user logged in; the switch IP address; and the current date and time. • A standard menu bar. Refer to Table 2: Menu Bar Elements on page 9 for additional details. This pane remains consistent across all views.
Workspace	Displays the information and work area for the different ScreenPlay features. All features are accessed via the menu bar with any subordinate functions, usually available through tabs. Each work area is described in sections to follow. At the top of the pane is a status bar that displays the current activity or condition, such as Successfully Fetched SNMP Details! or an error message, such as Unknown tag "test3".mismatched tag.

From the device dashboard, you can navigate to any other portion of the interface. The functions available in ScreenPlay are divided into three major categories:

- Configuration, which covers configuration of ports, VLANs, stacking, SNMP and dynamic ACLs.
- Statistics and Monitoring, which provides you with the capability to generate event logs, monitor and generate statistics on ports, and perform QoS monitoring.
- Administration, which allows you to perform administrative tasks on user accounts and user sessions and to issue CLI commands.

ScreenPlay Common Functions

This section describes those ScreenPlay functions that are displayed in all of the main workspaces (Dashboard, Configuration, Statistics & Monitoring and Administration). These include the following topics:

- Menu Bar
- Dashboard Switch Summary Icons
- Configuring the Refresh and Timeout and CLI Settings
- Customizing and Capturing the Tables

Menu Bar

The following table lists and describes the menu and sub-menu elements.

Table 2: Menu Bar Elements

Name	Description and Function
Dashboard	The opening screen that provides a one-glance snapshot of switch details, inventory, and management details. Refer to ScreenPlay Dashboard on page 7.
Configuration:	
Ports	Lists and describes the ports. A Port Details panel provides the capability to make certain modifications to the port configuration. Refer to Configuration--Ports on page 14.
VLANs	Lists and describes the VLANs. A VLAN Details panel provides the capability to make certain modifications to the VLAN configuration. Refer to Configuration--VLANs on page 18.
Stacking	Displays the stacking topology diagram and stacking configuration details. This submenu is enabled only on switches that support stacking. Refer to Configuration--Stacking on page 21.
SNMP	Lists SNMP settings, statistics, users and trap receivers. Refer to Configuration--SNMP on page 22.
Dynamic ACLs	Lists the dynamic ACLs on the switch. Provides the capability to create, edit and apply an ACL to an interface. Refer to Configuration--Dynamic ACLs on page 24.
Statistics and Monitoring:	
Event Log	Provides an event log of the activity on the switch, showing date, time, and type of event. Refer to Statistics and Monitoring--Event Log on page 27.
Ports	Provides port statistics and utilization details in tables and charts. Refer to Statistics and Monitoring--Ports on page 28.
QoS	Displays QoS (Quality of Service) profile information for each port. Refer to Statistics and Monitoring--QoS on page 30.
Administration:	
User Accounts	Lists user account information and provides the capability to create and modify the settings locally and with RADIUS and TACACS. Refer to Administration--User Accounts on page 32.
User Sessions	Lists information on the current session and provides a history of recent session activity. Refer to Administration--User Sessions on page 35.
CLI Shell	Provides the capability to issue CLI commands from within the application. Refer to Administration--CLI Shell on page 36.
Help:	
Services & Technical Support	Opens the Services and Support page on Extreme Networks' web site. www.extremenetworks.com/services/services-hub.aspx
EXOS Command Reference Guide	Links to a PDF copy of the current ExtremeXOS Command Reference Guide. **Note:** Please visit the Extreme Networks website for the latest version of ExtremeXOS documentation.

Table 2: Menu Bar Elements (continued)

Name	Description and Function
EXOS Concepts Guide	Links to a PDF copy of the current ExtremeXOS Concepts Guide. Note: Please visit the Extreme Networks website for the latest version of ExtremeXOS documentation.
About	Displays client environment information.
Logout	Exits ScreenPlay.
Save Config	A command button used to save configuration changes. When changes have been made, the button turns orange indicating that a saving action is required to permanently change the configuration.

Dashboard Switch Summary Icons

The following lists and describes the icons used on the Dashboard Switch Summary pane.

Icons	Description
	Slot—Operational, Failed, and Empty
	Fan Tray—Operational and Empty
	Power Supply—Powered on, Failed, and Empty

Point to an icon to show the unit type and state. Click the icon to show additional inventory information. The figure below shows two examples of the content.

Figure 3: Unit Information Screen

Configuring the Refresh and Timeout and CLI Settings

Following are the defaults for the following refresh, timeout and CLI settings:

General Refresh Interval	Default is 15 seconds.
Web Service Timeout	Default is 45 seconds.
Idle Timeout	Default is 10 minutes. (A warning is given one minute before.)
CLI Shell Background	Choose a color from the color palette. Default is white.
CLI Shell Foreground	Choose a color from the color palette. Default is black.
CLI Shell Port	Specify a port.

To reset these settings, use the following procedure:

1. Right-click almost any part of the ScreenPlay window to display one of two menus that have a Show Console choice.
2. From the menu, choose Show Console.

   A console pane is displayed at the bottom of the Dashboard, Configuration, Statistics & Monitoring, or Administration windows.
3. Click the Configuration tab as shown in the figure below.

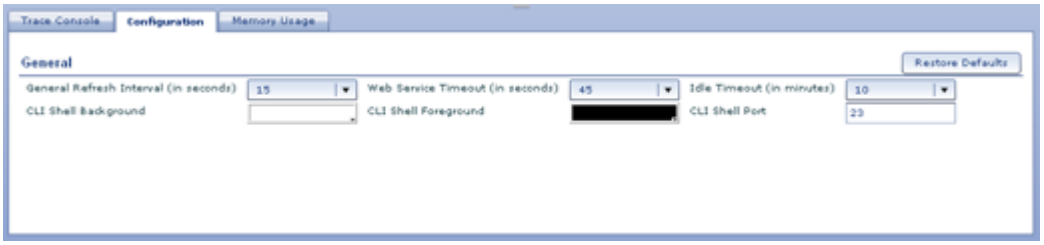


Figure 4: Console—Configuration Tab

4. From the appropriate drop-down menu, choose another setting for any or all of the first five selections or enter a port number in the CLI Shell Port text box.
5. To restore the original default settings, click the Restore Defaults command button.

Customizing and Capturing the Tables

ScreenPlay allows you to customize the format of a table and then print it or copy it to another application such as Microsoft Excel®. Copy the table to another application by clicking the copy icon , opening the target application and pasting in the table.

- Resize the column width using standard column resizing bars between the heading cells.
- Sort rows by clicking in a table heading cell to display an up or down arrow tip.
- Remove columns by clicking the hide icon and in the displayed Select Columns box, clear the unwanted column name(s).
- Select specific row entries by typing the relevant text into the search field . Entries that do not include the text are hidden.

- Print an original or modified table by clicking the print icon located just above the table.

  A standard print box opens. This icon prints the specific table only and prints it as it appears on the screen; if any cell contents are hidden on the screen, they are hidden on the printed copy. To print the entire screen, use the browser print command.

- Copy the table to another application by clicking the copy icon, opening the target application and pasting in the table

Dashboard Workspace

The Dashboard workspace contains three segments: Inventory Information; Management; and Switch Details. These are displayed in Figure 5 and are described in the table that follows it.

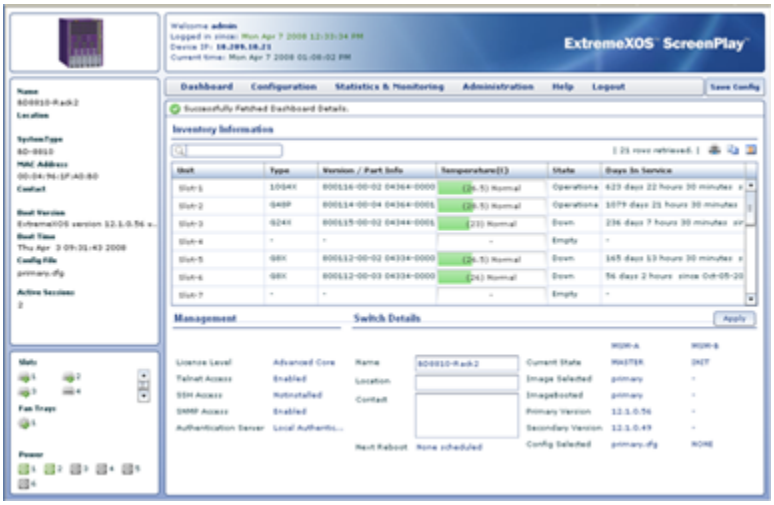


Figure 5: Dashboard

Screen/Pane	Description
Inventory Information	Provides information about the hardware units: the type of system; the running temperature with a colored indicator; and the total number of days that the switch has been in service. Click the different unit to display additional information, examples of which are shown in the above figure. Allows for customizing and capture of the table.
Management	Displays the availability/status of configuration elements: license level; Telnet access; SSH Access; SNMP Access; and Authentication Server.
Switch Details	Describes the current condition of the switch including its location, software version, state, and configuration. Allows for the modification of the switch name, location and contact.

4 Configuration

Configuration--Ports
Configuration--VLANs
Configuration--Stacking
Configuration--SNMP
Configuration--Dynamic ACLs

You can use the ScreenPlay tool to perform device-level configuration tasks. This section provides an overview of the five configuration panes available through ScreenPlay:

- Ports
- VLANs
- Stacking
- SNMP
- Dynamic ACLs

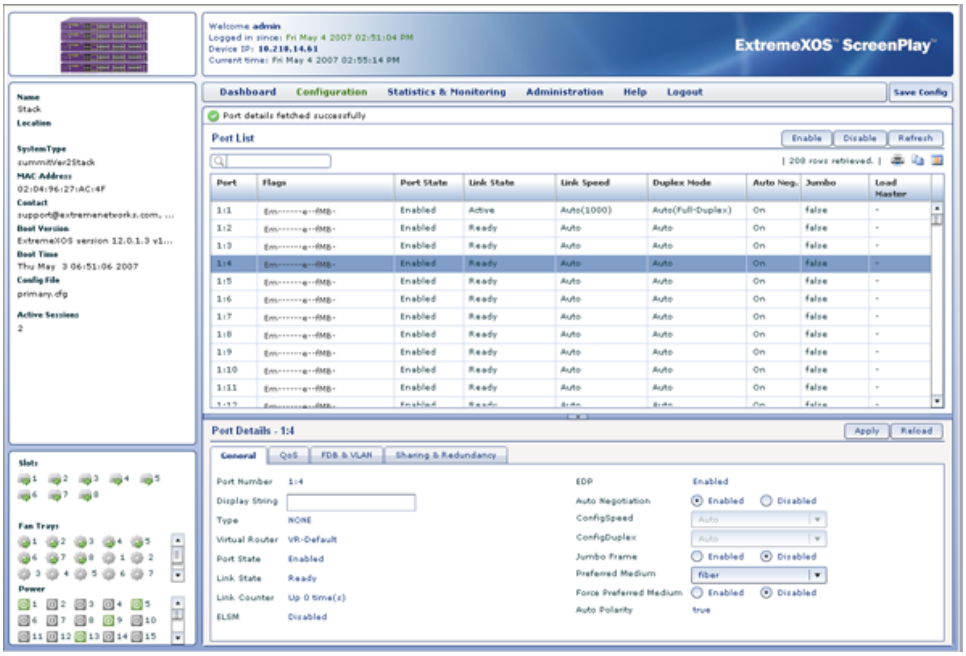
Configuration--Ports

This feature allows you to view and modify some of the basic configurations of the ports on the device. The topics available through the ports configuration screen are:

- Port list
- Port details
- Enabling and disabling ports
- Basic port set operations

Modifying Single Ports

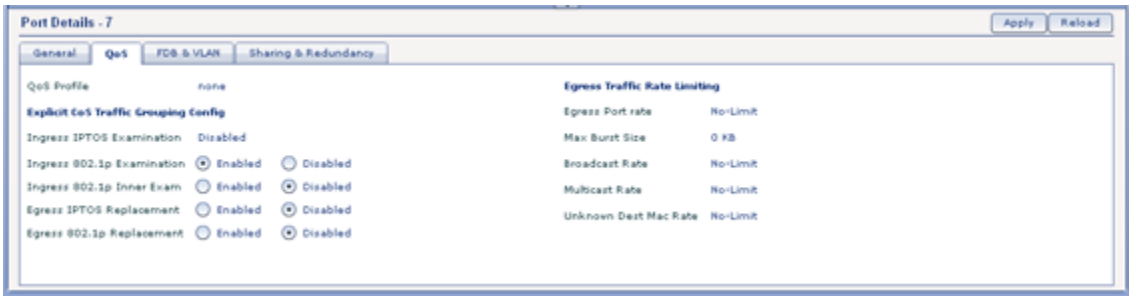
The following shows the **Ports Configuration** screen. Click one of the ports in the **Port List** to show the Port Details information for that port. Port Details information is displayed under four tabs. The **General details** tab information is displayed in Figure 6: Ports Configuration Screen with Single Port Details on page 15, and the other **Port Detail** tabs follow.



Screen/Pane	Description
Port List	Lists the ports and their respective Flags (see Figure 11), Port State, Link State, Link Speed, Duplex Mode, Auto Negotiation, Jumbo frames and Load Master. Allows customizing and capture of the table. Ports can be Enabled and Disabled using the command buttons.
Port Details for the Selected Port	Displays details for the port that is selected from the Port List.
General Tab	Displays the Port Number and Type, settings for the Virtual Router, Port State, Link State, Link Counter, ELSM, EDP and Auto Polarity. Allows modifications to Auto Negotiation, ConfigSpeed, ConfigDuplex, Jumbo Frame, Preferred Medium and Force Preferred Medium

Figure 6: Ports Configuration Screen with Single Port Details

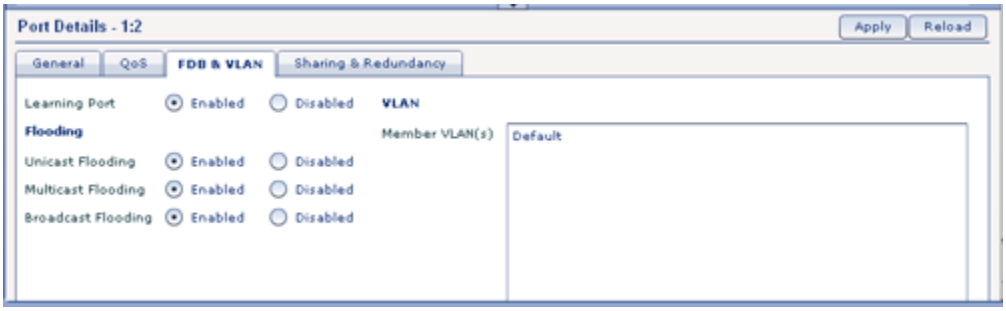
Figure 7: Port Details—QoS on page 15 displays the QoS details tab, and the table below it describes its elements.



Screen/Pane	Description
QoS Tab	Displays the QoS Profile name, Egress Traffic Rate Limiting setting: Egress Port rate, Max Burst Size, Broadcast Rate, Mulitcast Rate, Unknown DestMac Rate and Ingress IPTOS Examination. Allows the Explicit CoS Traffic Grouping Config settings: Ingress 802.1p Examination; Ingress 802.1p Inner Exam; Egress IPTOS Replacement; and Egress 802.1p Replacement to be enabled or disabled.

Figure 7: Port Details—QoS

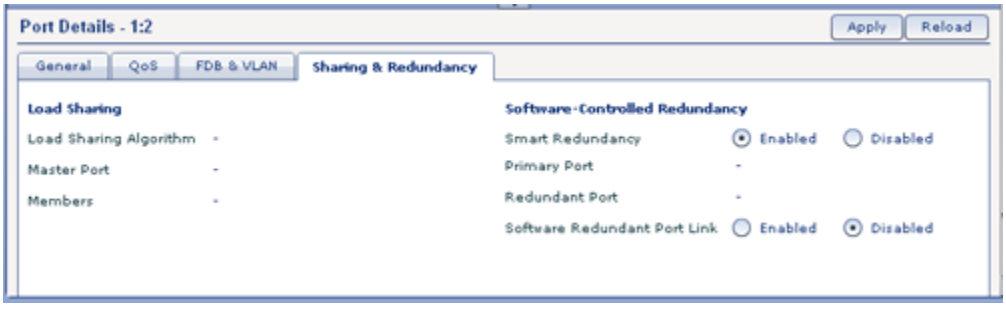
Figure 8: Port Details—FDB & VLAN on page 16 displays the FDB & VLAN details tab, and the table below it describes its elements.



Screen/Pane	Description
FDB & VLAN Tab	Displays the VLANs. Allows the learning port and unicast, multicast and broadcast flooding to be enabled or disabled.

Figure 8: Port Details—FDB & VLAN

Figure 9: Port Details—Sharing and Redundancy on page 16 displays the Sharing & Redundancy details tab, and the table below it describes its elements.



Screen/Pane	Description
Sharing & Redundancy Tab	Displays Load Sharing: Load sharing/link aggregation algorithm, Master Port and Members.

Screen/Pane	Description
	On modular switches and SummitStack, displays Software-Controlled Redundancy, the Primary and Redundant Ports, and allows Smart Redundancy and Software Redundant Port Link to be enabled or disabled.

Figure 9: Port Details—Sharing and Redundancy

Modifying Multiple Ports

To show Port Details for multiple ports, Ctrl + click two or more ports in the Port List. The resulting Port Details are shown in the figure below and the table below it describes its elements.

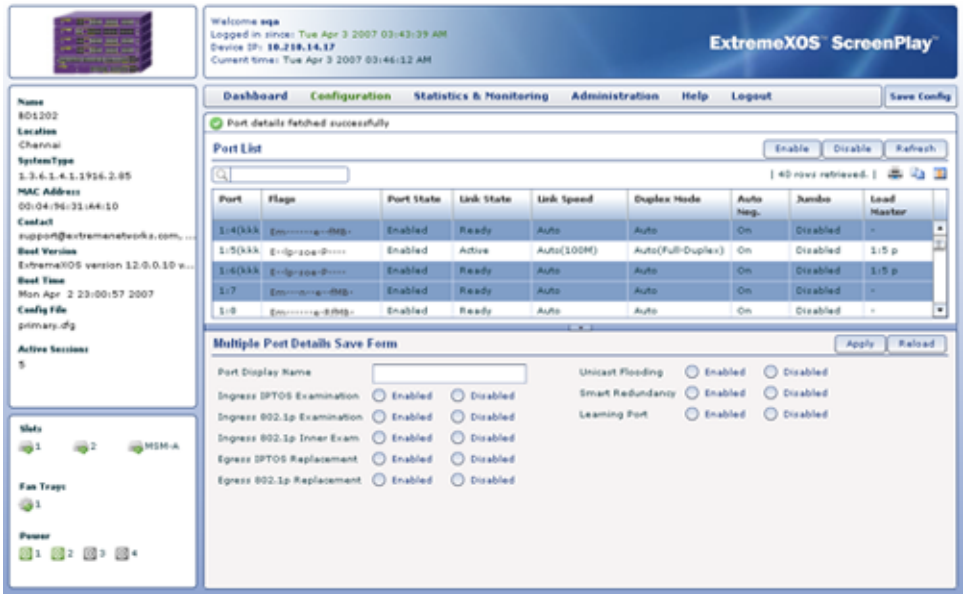


Figure 10: Ports Configuration Screen with Multiple Port Details

Screen/Pane	Description
Multiple Port Details Save Form	Displays details for two or more ports selected from the Port List. Allows a Port Display Name to be provided and Ingress IPTOS Examinations, Ingress 802.1p Examinations, Ingress 802.1p Inner Exam, Egress IPTOS Replacements, Egress 802.1p Replacement, Unicast Flooding, Smart Redundancy, and Learning Port to be enabled or disabled.

Click one of the entries in the Port List Flags column to display the Flags Legend. The settings in the list that apply to the particular port are displayed in bold print as shown in the figure below.

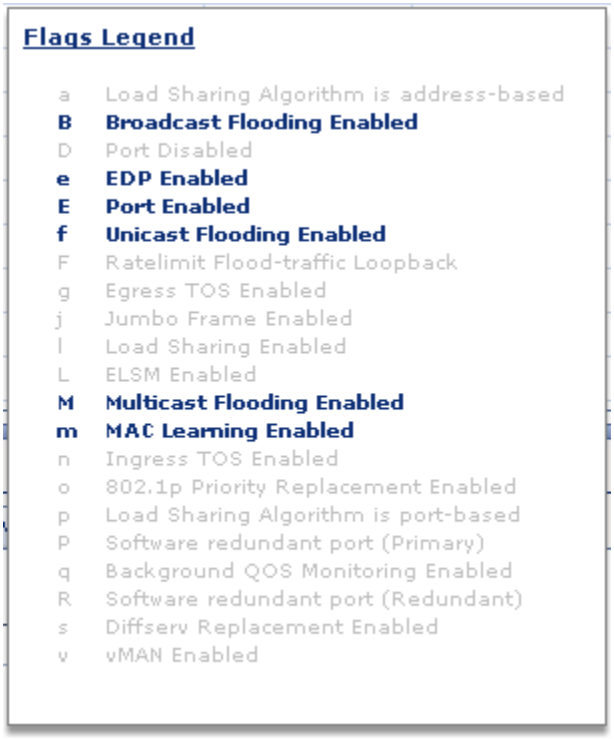

Flags Legend
a Load Sharing Algorithm is address-based
B Broadcast Flooding Enabled
D Port Disabled
e EDP Enabled
E Port Enabled
f Unicast Flooding Enabled
F Ratelimit Flood-traffic Loopback
g Egress TOS Enabled
j Jumbo Frame Enabled
l Load Sharing Enabled
L ELSM Enabled
M Multicast Flooding Enabled
m MAC Learning Enabled
n Ingress TOS Enabled
o 802.1p Priority Replacement Enabled
p Load Sharing Algorithm is port-based
P Software redundant port (Primary)
q Background QOS Monitoring Enabled
R Software redundant port (Redundant)
s Diffserv Replacement Enabled
v vMAN Enabled

Figure 11: Flags Legend—Configuration

Configuration--VLANs

This feature allows you to create, modify, and delete VLANs, add ports to VLANs and configure them. The topics available through the VLAN configuration screen are:

- VLAN list
- VLAN details (click one of the VLANs in the list)
- Enabling and disabling VLANs
- Basic VLAN configuration
- Port membership in VLANs

The figure below shows the VLAN configuration screen of the ScreenPlay tool and the table below it describes its elements.

Click one of the VLANS in the VLAN List to show the VLAN Details information for it. The General tab is displayed in the figure below; the other tabs follow.

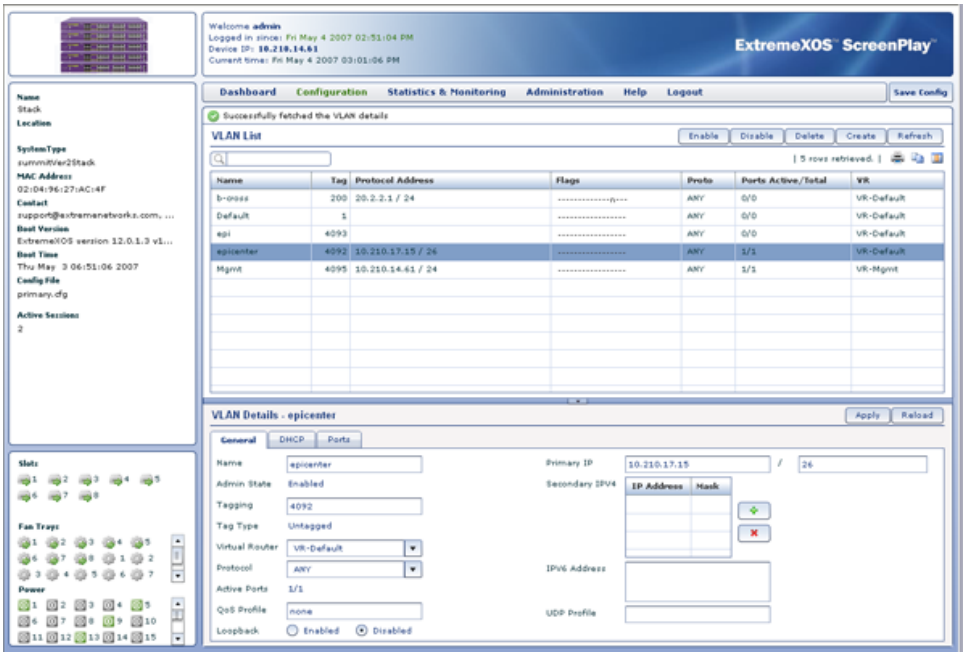


Figure 12: VLANs Configuration Screen

Screen/Pane	Description
VLAN List	Lists the VLANs and their respective names, Tags, Protocol Addresses, Flags, Protocol filters, Active and Total Ports, and Virtual Routers. Allows VLANs to be created, deleted, enabled, disabled, The table can be customized and captured and manually refreshed.
VLAN Details	Displays information for the VLAN selected from the VLAN List.
General	Displays: Admin State, Tag Type, and the Active Ports. Allows modification to: Name, Tagging, Virtual Router, Protocol filters, QoS Profile, Loopback Primary IP, Secondary IPv4, IPv6 Address and the UDP Profile.

The figure below displays the DHCP (Dynamic Host Configuration Protocol) tab, and the table below it describes its elements.

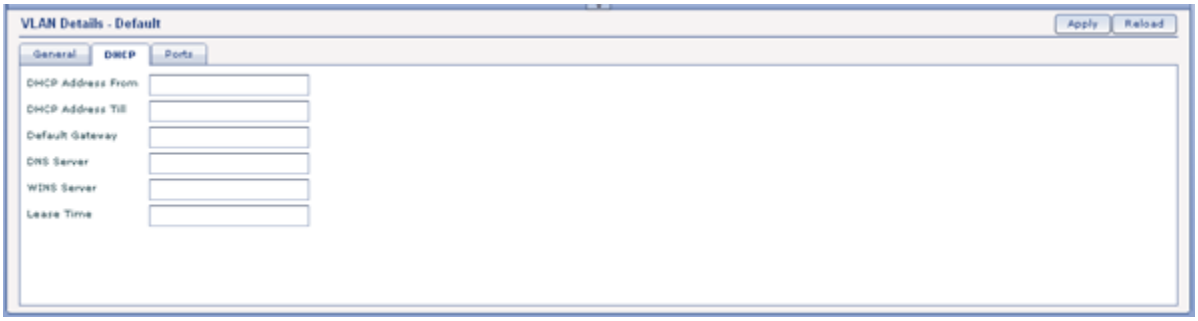


Figure 13: Configuration—VLAN Details—DHCP

Screen/Pane	Description
DHCP	Allows modification to: DHCP (Dynamic Host Configuration Protocol) Address, Default Gateway, DNS (Domain Name Servers) Server, WINS (Windows Internet Naming Service) Server, and Lease Time.

The figure below displays the **Ports** tab, and the table below it describes its elements.

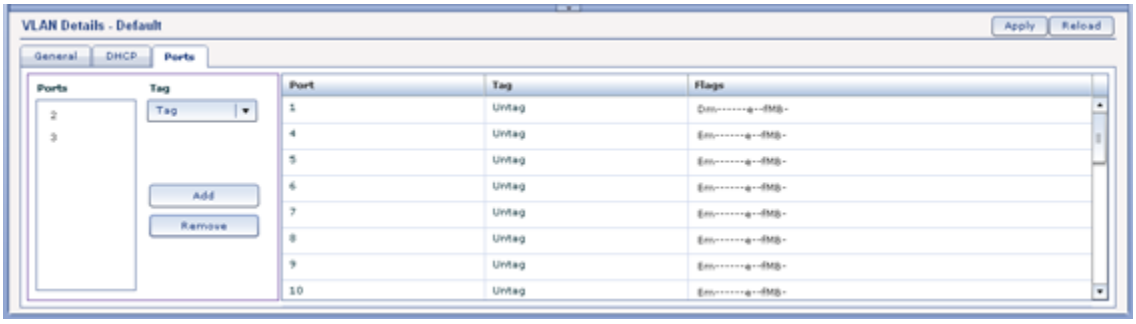


Figure 14: Configuration—VLAN Details—Port

Screen/Pane	Description
Ports	Displays the Flags assigned to the port. Refer to Figure 11: Flags Legend—Configuration on page 18. Allows ports to be added and removed, and tagged and untagged. In the Ports panel, point to a port number to display its Port Properties. In the Flags column, point to flag to display the Flags Legend.

VLAN Configuration Procedures

Following are common procedures for using VLAN Configuration functions.

Creating VLANs

To create a VLAN:

1 From the **VLAN List** screen, click the **Create** command button.

The **New VLAN Details** pane is displayed. (This pane matches that shown in Configuration--VLANs on page 18).

2 Type in the required information.

3 To save the configuration, click the **Save** command button.

The VLAN is saved to the switch.

4 Click the **Save Config** command button to permanently save the new VLAN.

Deleting VLANs

To delete a VLAN:

1 From the VLAN List screen, click the name of the VLAN to be deleted.

The VLAN Details pane is displayed for the selected VLAN.

2 Click the Delete command button.

The VLAN is deleted and the action is confirmed.

Configuration--Stacking

This feature allows you to manage, view, and monitor ExtremeXOS stackable switches in a stack configuration. The feature is limited to viewing the node configuration and monitoring the stack topology and interconnectivity among the stack members. The configuration capabilities of actually setting up or maintaining a stack are outside the scope of this feature.

The features available through the stacking configuration screen are:

- Stack topology
- Stack nodes and connectivity
- Stack slot details

Note

This feature is available only on switches that support stacking. When the switch does not support stacking, the submenu is grayed out.

The figure below shows the stacking configuration screen of the ScreenPlay tool, and the table below it describes its elements.

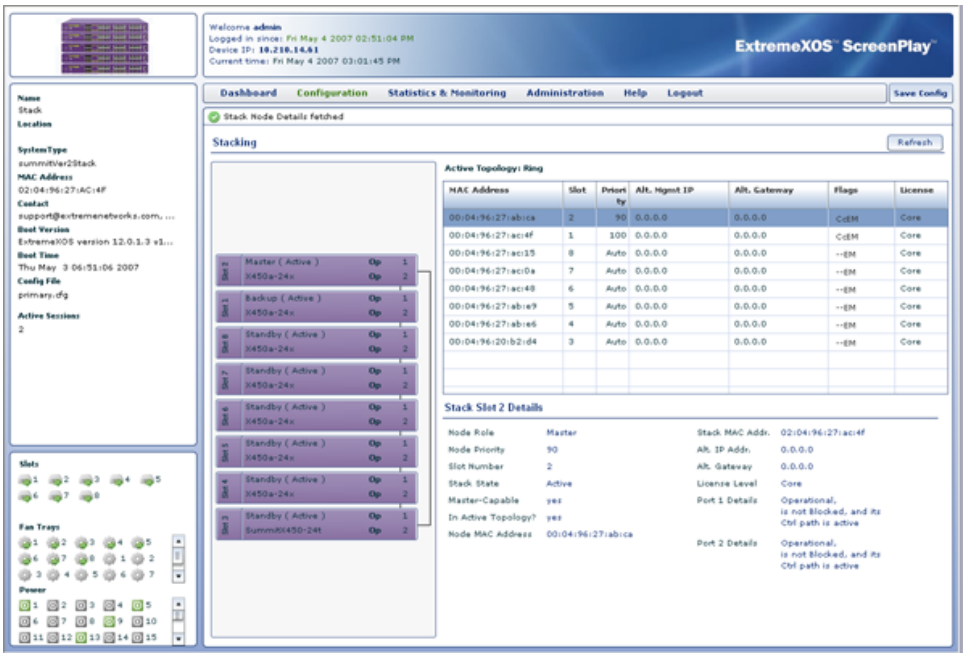


Figure 15: Stacking Configuration Screen

Screen/Pane	Description
Stacking	Displays the active topology for the stack (ring or daisy chain) and for each node: the MAC address, the slot number in use, the priority used in node role election, alternate management IP address, alternate gateway, flags (point to a flag to display the Flags Legend) and the license.
Stack Slot Details	Displays configuration and status information for the slot that is selected in the Stacking list.

Configuration--SNMP

This feature allows you to view the SNMP configuration on the switch. The information provided is useful to view the settings that are used by an SNMP client communicating with the switch. The tool allows you to view and manipulate the following SNMP features:

- SNMP settings
- SNMP v1 and v2c communities
- SNMP v3 users
- SNMP trap receivers
- SNMP statistics

Note
There are no capabilities to make changes to the SNMP configuration in this release.

The figure below shows two SNMP configuration screens that display the content under all of the tabs. The table below the figure describes its elements.

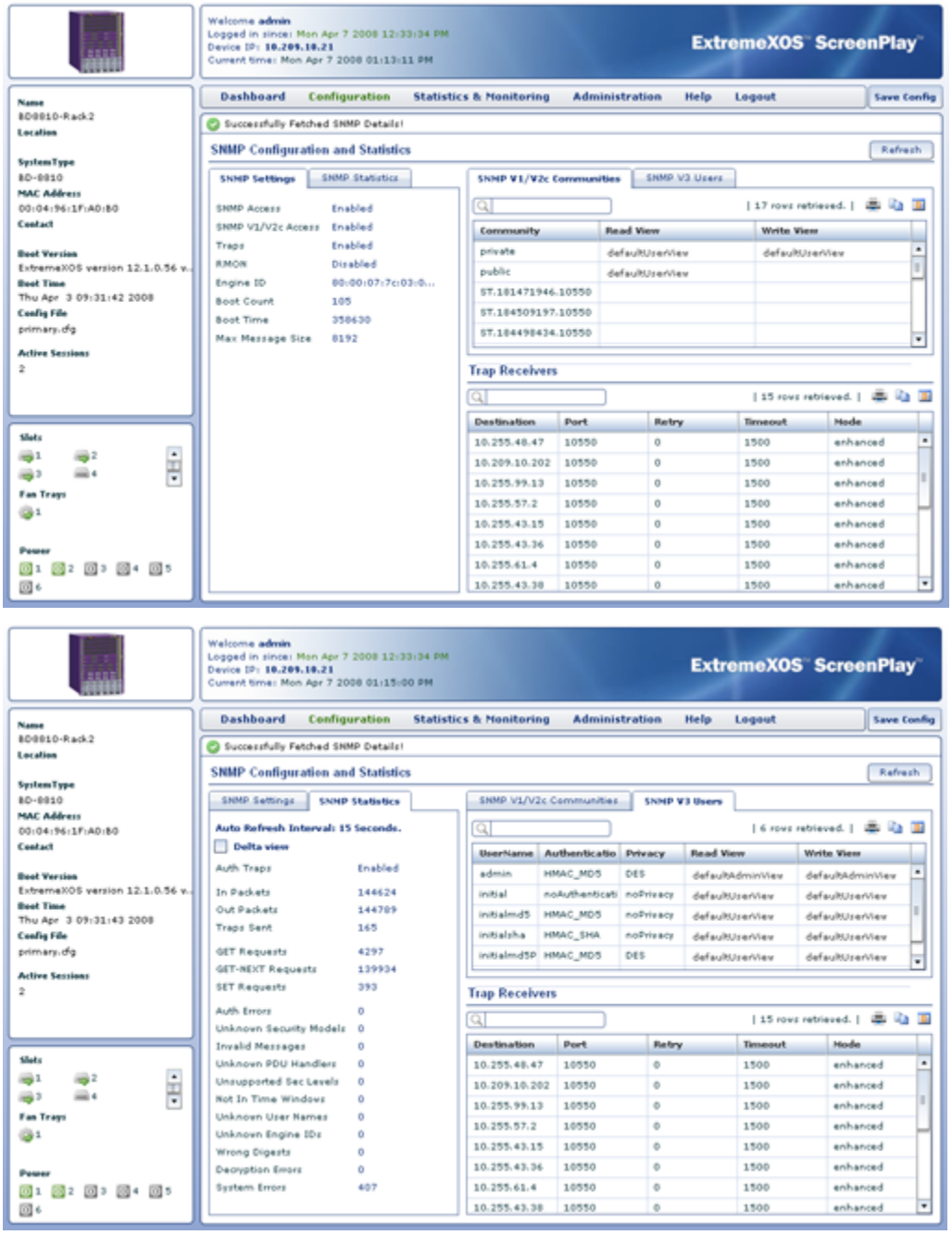


Figure 16: SNMP Configuration Screens

Screen/Pane	Description
SNMP Settings	Displays SNMP configuration settings and access status.
SNMP Statistics	Displays SNMP statistics. Move the cursor over each item in the list to show a tool tip with additional explanation of each. Clicking the Delta view box starts a count up of new actions beginning from the time the box is checked. The start time is displayed.

Screen/Pane	Description
SNMP V1/V2c Communities	Lists the community strings and the type of access. Click the entries in the Read View and Write View columns to see the MIB Object Identifiers (OIDs) that are included and excluded. Allows for customizing and capture of the table, and a manual Refresh function.
SNMP V3 Users	Lists the users, authentication method, privacy status, and type of access. Click the entries in the Read View and Write View columns to see the MIB OIDs that are included and excluded. Allows for customizing and capture of the table, and a manual Refresh function.
Trap Receivers	Lists the trap receiver IP addresses, Port, number of retrys, Timeout, and the Modes (enhanced or standard). Allows for customizing and capture of the table.

Configuration--Dynamic ACLs

This feature allows you to manage dynamic ACLs. It provide a process that is easier than the long command line syntax from the CLI. The following functionality is included.

- Displays the ACLs currently existing on the switch
- Creates and edits ACLs
- Applies a completed ACL to an interface.

The figure below shows a dynamic ACL screen, and the table below it describes its elements.

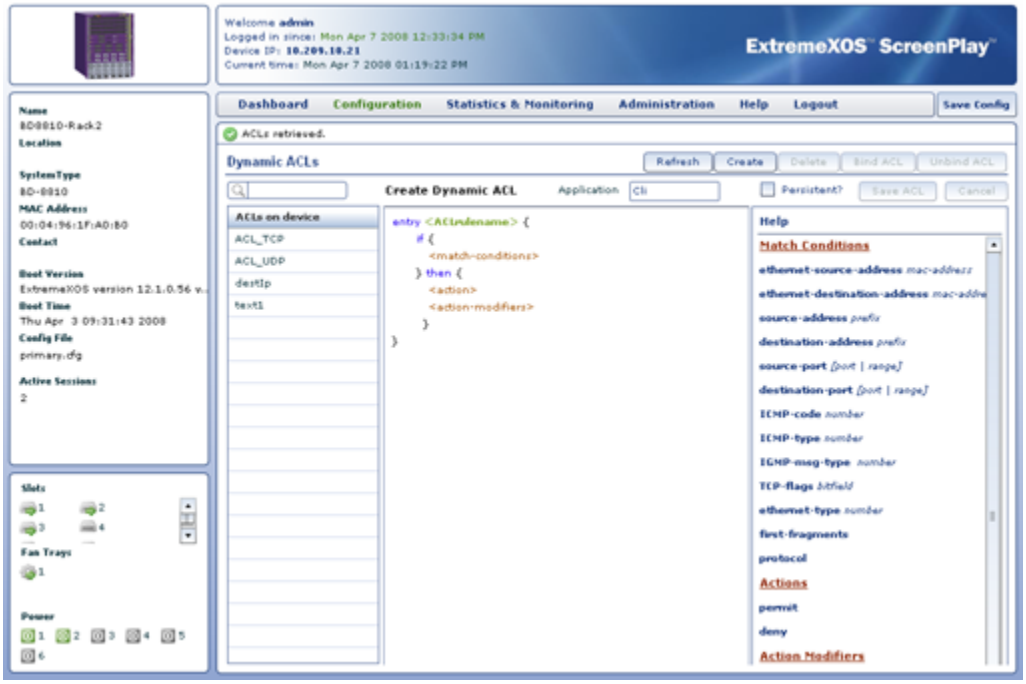


Figure 17: Creating a Dynamic ACL

Screen/Pane	Description
ACLs on device	Displays the ACLs that are currently available on the switch.
Create Dynamic ACL	Displays an template on which to create an ACL. (See the following procedures.)
Help	Contains interactive lists of Match Conditions, Actions, and Action Modifiers used to create an ACL.

Creating ACLs

To create an ACL:

1. Click the **Create** button to display a new ACL template in the **Create Dynamic ACL** pane.
2. Replace **<ACLrulename>** with a name.
3. In the template, click in **<match-conditions>** and then click one of the March Conditions listed in the **Help** pane.

   The selection is inserted into the template.
4. Repeat for the other elements as necessary.
5. Click the **Save ACL** button.

   The new ACL is saved and added to the ACLs on device pane.

Applying ACLs to Interfaces

To apply an ACL to an interface:

1. In the **ACLs on device** pane, click the ACL to be applied.

   The Bind ACL command button is enabled.
2. Click the **Bind ACL** button. The **Apply <ACL name> on** interface pane is displayed.
3. Click one of the three interface radio buttons (**Any**, **Ports** or **Vlans**). The appropriate fields for the particular interface are displayed and enabled. (See the figure below.)
   - Clicking **Any** disables the other controls in the pane.
   - Clicking **Ports** displays a list of all ports on the device. You can choose one or more ports.
   - Clicking **Vlans** displays a text box. Enter a VLAN name in the box.

   If there are other ACLs applied to the chosen interface, you can apply the new ACL as either the “first” or “last” ACL or position it before or after an ACL that is already applied to the interface. If the ACL is already applied to the chosen port or VLAN, all controls are disabled.
4. Make the selections and **Save**.

   The ACL is applied to the interface(s) and the details are displayed in the **Interfaces applied to** pane. Point to the ACL to display a tooltip showing the interface status.

Removing ACLs

First unbind the ACL from the interface, if appropriate, and then remove it from the device.

1 In the ACLs on device pane, click the ACL to be removed. The interface details in the Interfaces applied to pane and displayed. Enable the Unbind ACL command button by clicking the interface details row.

   a You can choose multiple ports to unbind at the same time but only one VLAN. To unbind all interfaces at once, click the Select All box.

   b Click Unbind ACL.

2 In the ACLs on device pane, click the ACL to be removed then click the Delete button.

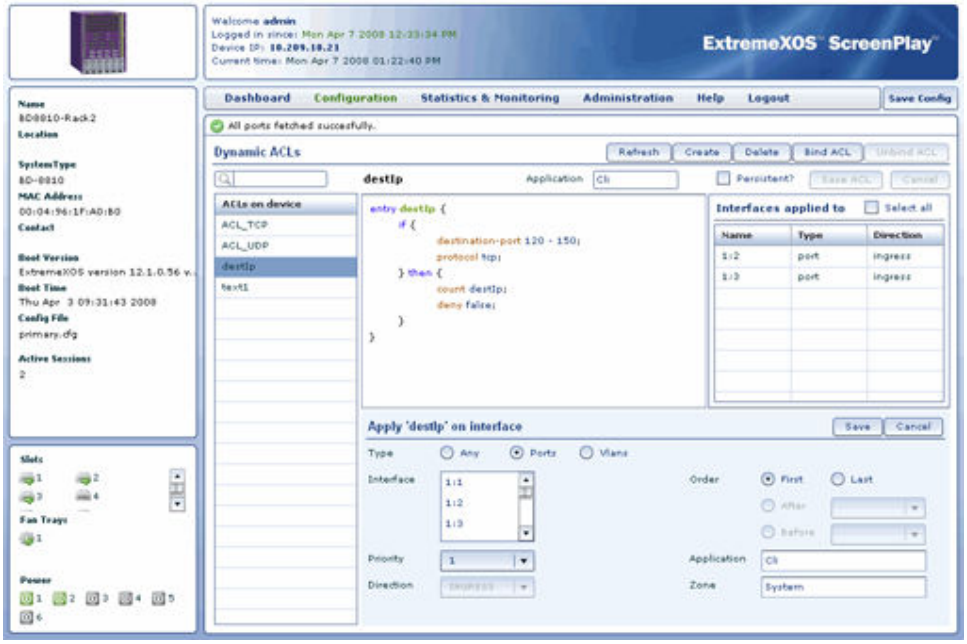


Figure 18: Applying an ACL to an Interface

Screen/Pane	Description
Apply <ACLrulename> on interface	Allows you to choose the interface to which the dynamic ACL is to be applied as well as priority, direction, order, application, and zone.
Interfaces applied to	Displays the interfaces to which the ACL selected in the ACLs on device pane is bound.

5 Statistics and Monitoring

Statistics and Monitoring--Event Log
Statistics and Monitoring--Ports
Statistics and Monitoring--QoS

This section provides an overview of the three statistics and monitoring panes available through ScreenPlay:

- Event Log
- Ports
- QoS

Statistics and Monitoring--Event Log

This feature provides a tabular event log of the activity on the switch. The figure below shows the Event Log screen of the ScreenPlay tool, and the table below it describes its elements.

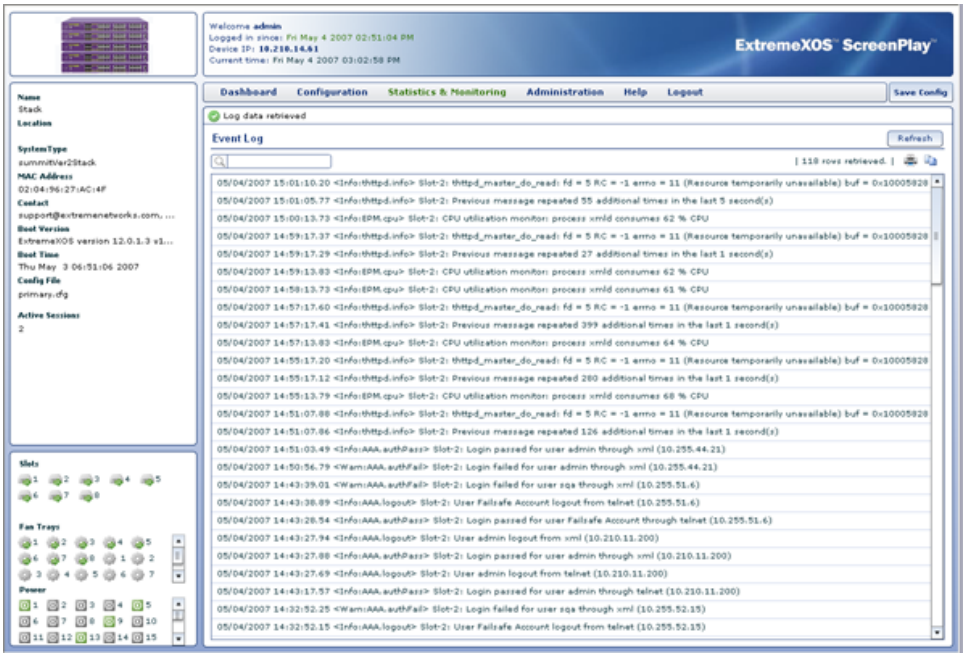


Figure 19: Statistics & Monitoring—Event Log Screen

Screen/Pane	Description
Event Log	Displays the date, time and type of event. Allows for customizing and capture of the table and a manual Refresh function.

Statistics and Monitoring--Ports

This feature allows you to view the live statistics of the ports as various kinds of charts and tables. The charts and tables are viewed in the following tabbed screens:

- Utilization Chart
- Statistics Table
- Bandwidth Charge

The figure below shows the Utilization Chart tab information, and the table below it describes its elements.

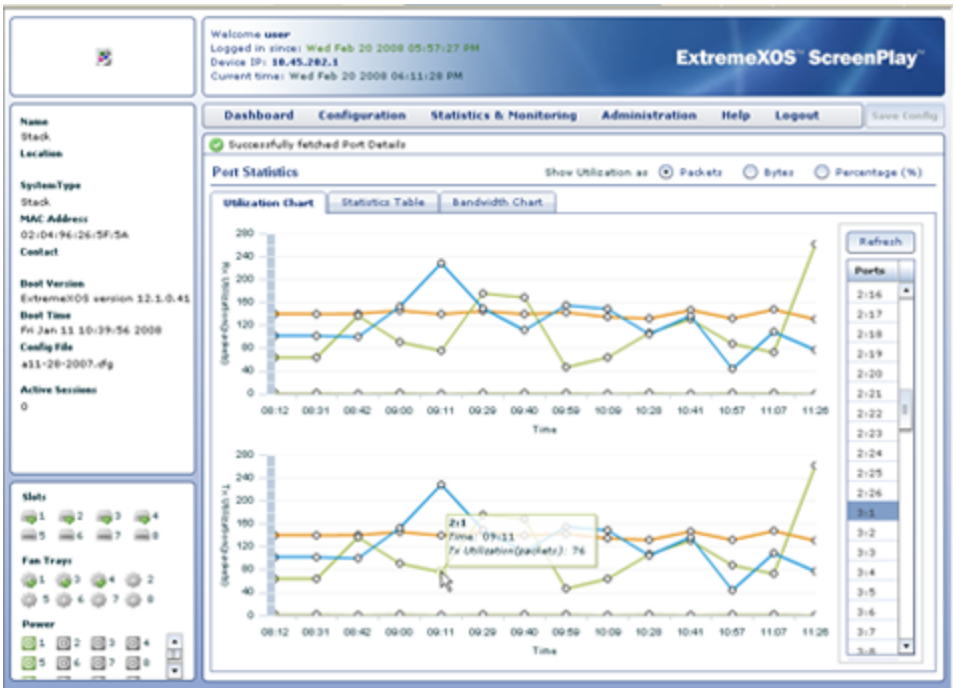


Figure 20: Statistics & Monitoring—Port Statistics—Utilization Chart Screen

Screen/Pane	Description
Utilization Chart	Graphically displays port utilization, received and transmitted. Allows the graph to be plotted in bytes per second, packets per second or as a percentage of bandwidth. Point to any of the Port numbers to display a tool tip that shows the Port Properties: Display String and Link State. Point to one of the plot points for more information.

The figure below shows the Statistics Table tab information, and the table below it describes its elements.

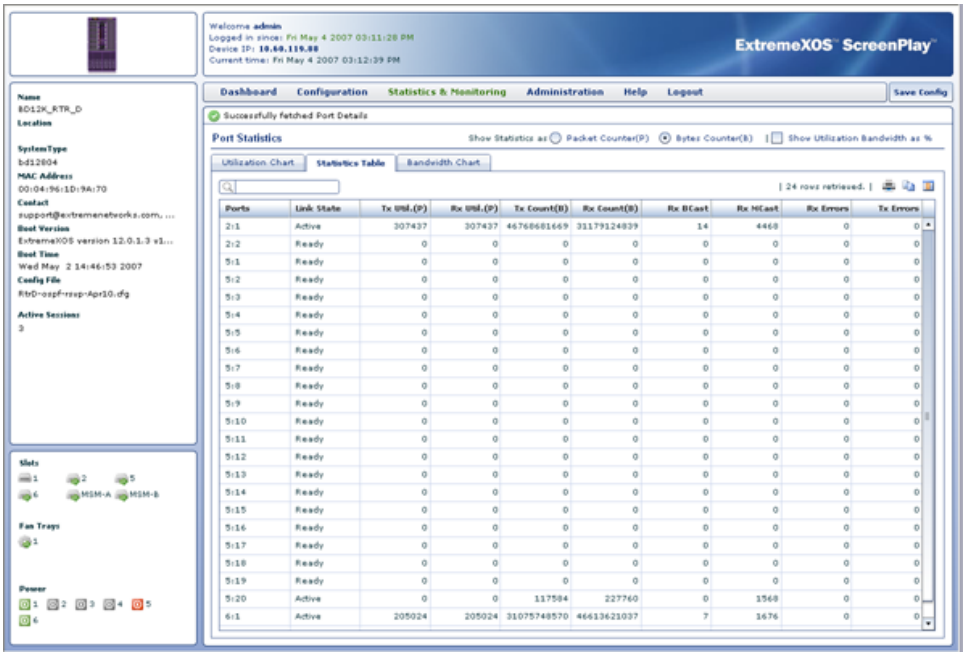


Figure 21: Statistics & Monitoring—Port Statistics—Statistics Table Screen

Screen/Pane	Description
Statistics Table	Lists the available ports and their link state, bandwidth utilization—as a number or percent—transmitted byte or packet count, received byte or packet count, received broadcast, received multicast, invalid frames received and transmitted. Use the radio buttons and check box to choose the display. Allows the table to be customized and captured.

The figure below shows the Bandwidth Chart, and the table below it describes its elements.

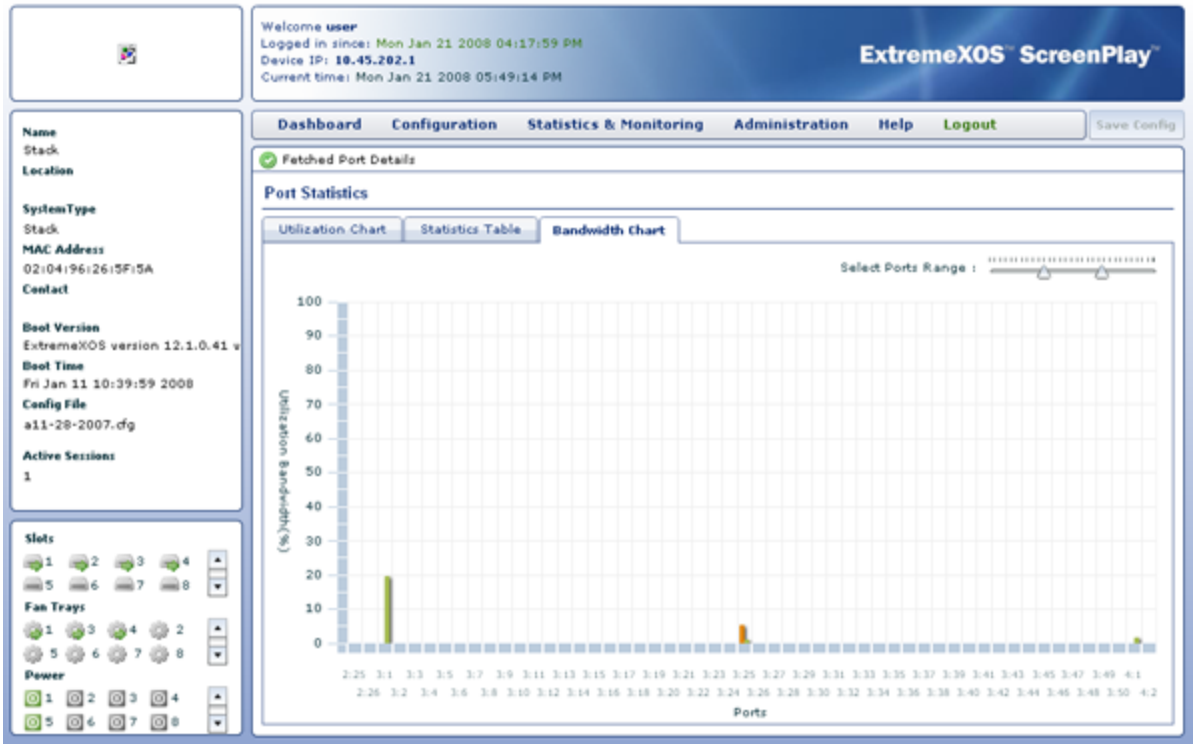


Figure 22: Statistics & Monitoring—Port Statistics—Bandwidth Chart Screen

Screen/Pane	Description
Bandwidth Chart	Displays in a bar chart, the percentage of bandwidth being utilized for each port. Allows the range of ports to be selected. Point to a bar to display its port number and Rx or Tx utilization percentage.

Statistics and Monitoring--QoS

This feature allows you to monitor QoS information on a port (both bytes and packets). The figure below shows the QoS Monitor screen, and the table below it describes its elements.

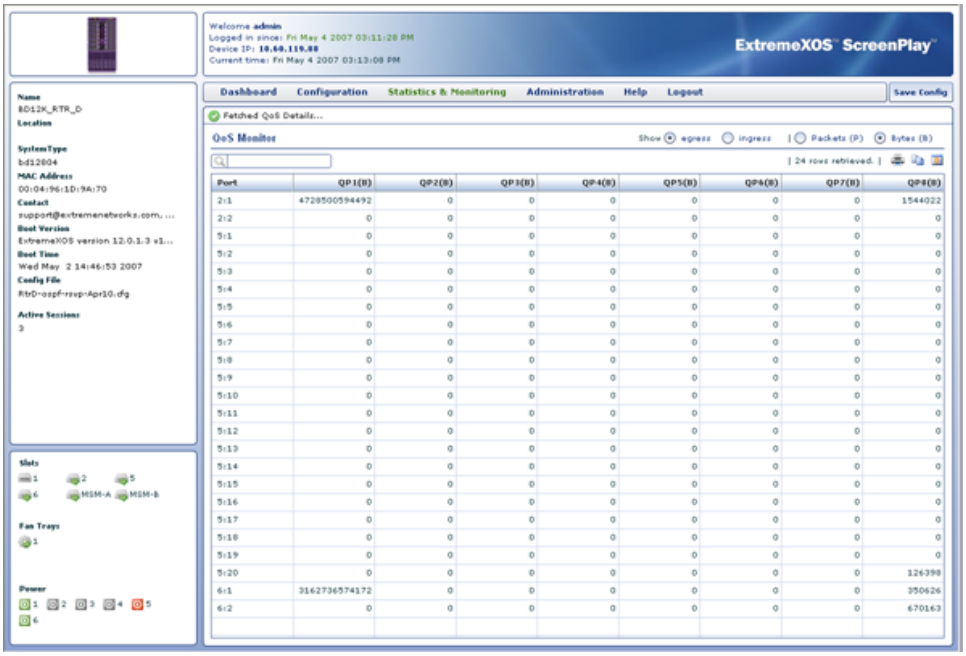


Figure 23: Statistics & Monitoring—QoS Monitor Screen

Screen/Pane	Description
QoS Monitor	Displays the QoS profiles assigned to each port. Allows the table to be shown in terms of egress or ingress, packets (P) or bytes (B), and for the table to be customized and captured.

6 Administration

Administration--User Accounts
Administration--User Sessions
Administration--CLI Shell

This section provides an overview of the administration panes available through ScreenPlay:

- Accounts
- Sessions
- CLI Shell

Administration--User Accounts

This feature allows you to manage user accounts on a switch. This includes the ability to add, modify and delete user accounts local to the switch and to configure remote RADIUS AAA or TACACS servers.

Information on the User Accounts screen is displayed under the following four tabs:

- Local Users
- Global Password Policy
- RADIUS
- TACACS

The figure below shows the Local Users screen of the Administrative section, and the table below it describes its elements.

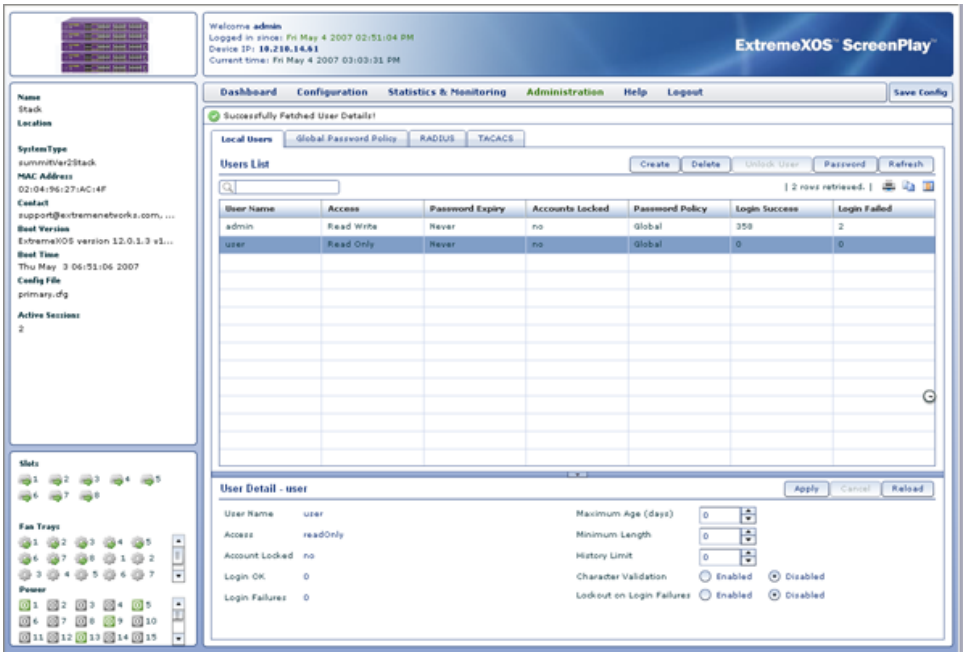


Figure 24: User Accounts—Local Users Screen

Screen/Pane	Description
Local Users Tab	Displays the users and information on their accounts Allows you to Create or Delete a user account, Unlock a user account and change a Password. The table can be customized and captured. The User Detail pane displays information on the user selected in the Users List and allows setting some limitations on the account.

The figure below shows the Global Password Policy screen of the Administrative section, and the table below it describes its elements.

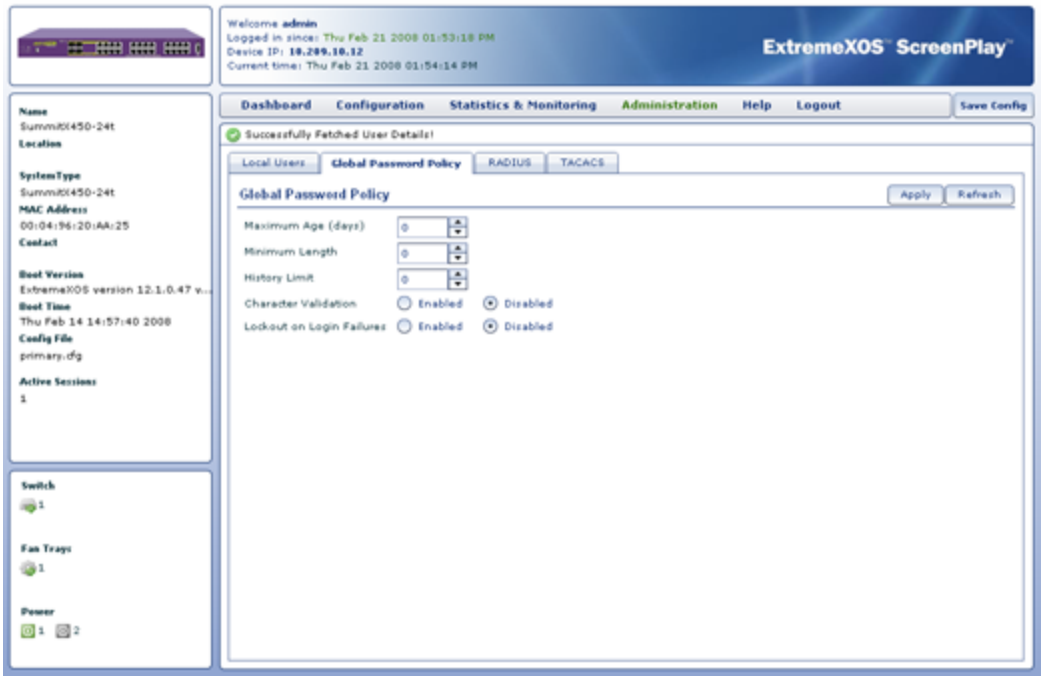


Figure 25: User Accounts—Global Password Policy Screen

Screen/Pane	Description
Global Password Policy Tab	Allows you to set limitations on passwords for all users.

The following figure shows the RADIUS screen, and the table below it describes its elements.

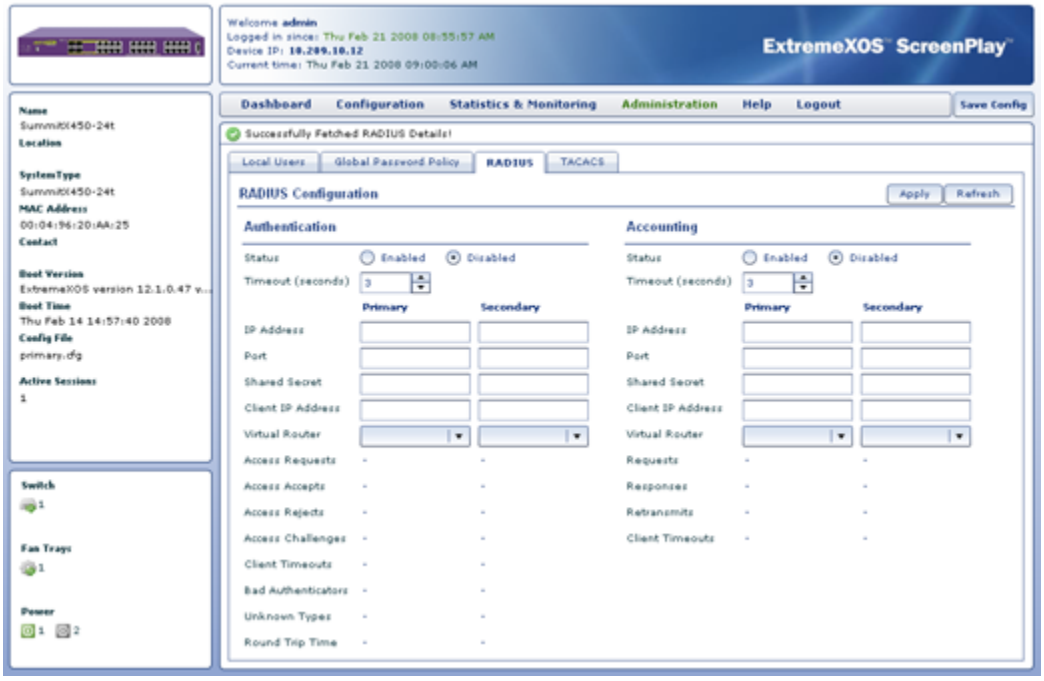


Figure 26: User Accounts—RADIUS Screen

Screen/Pane	Description
RADIUS Tab	Displays Authentication and Accounting information for both the Primary and Secondary servers. This includes numbers of various access and response events. Allows you to configure Status, Timeout, IP Addresses, Ports, Shared Secrets, Client IP Addresses and Virtual Routers.

The figure below shows the TACACS screen, and the table below it describes its elements.

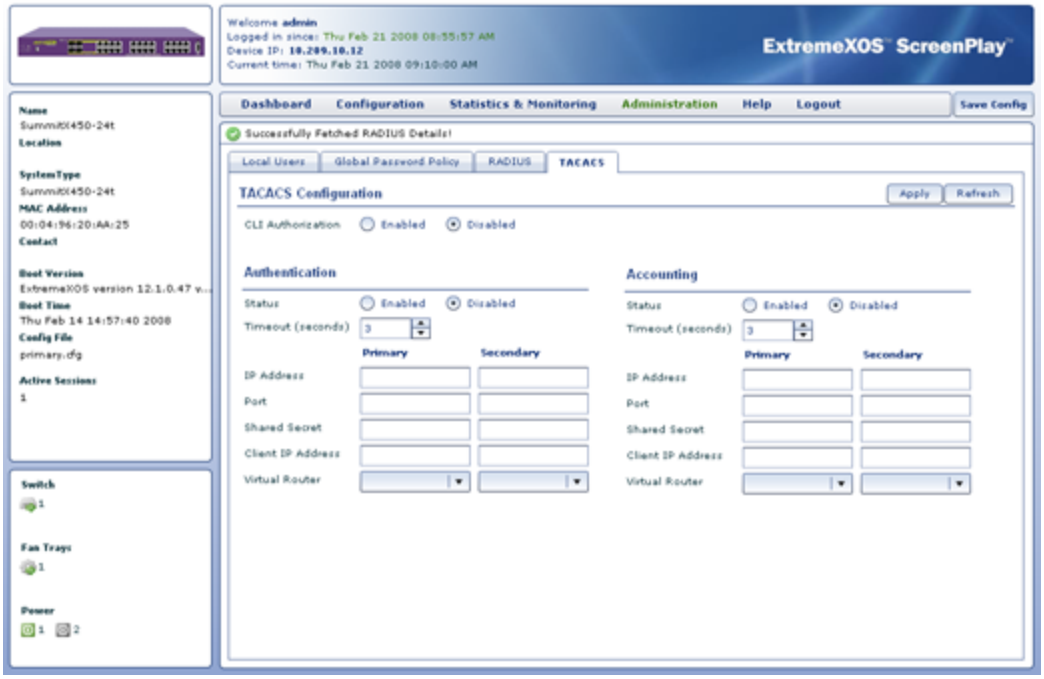


Figure 27: User Accounts—TACACS Screen

Screen/Pane	Description
TACACS Tab	Allows you to configure Status, Timeout, IP Addresses, Ports, Shared Secrets, Client IP Addresses and Virtual Routers for Authentication and Accounting Primary and Secondary servers.

Administration--User Sessions

This feature shows the list of SSH, XML, and Telnet sessions on the switch. It includes the ability to view current and historical sessions and allow administrators to kill rogue sessions. The features available through the sessions management screen are:

- Monitor and manipulate active CLI and XML API sessions
- Clear selected session
- View session history

The figure below shows the User Sessions screen of the ScreenPlay tool, and the table below it describes its elements.

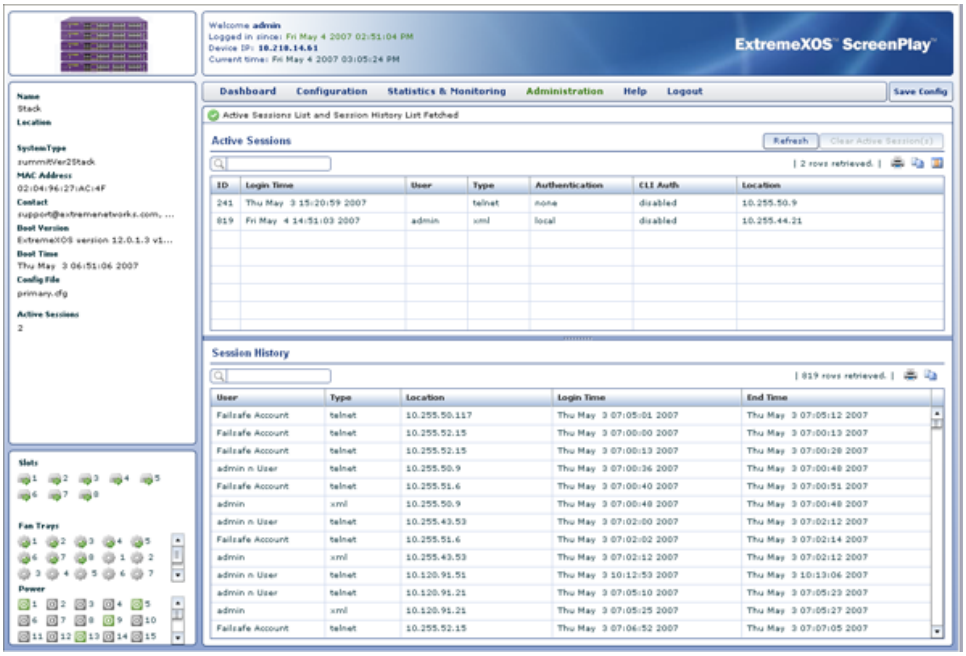


Figure 28: User Sessions Screen

Screen/Pane	Description
Active Sessions	Displays session number, login time, user name, type of connection, authentication, type of authentication if enabled, and the IP address from which the user is logged in. Allows the current session(s) to be cleared and the table to be customized and captured.
Session History	Displays the history of sessions showing: user name, type of connection, IP address from which the user was logged in and the login and logout times. Allows the list to be customized and captured.

Administration--CLI Shell

This feature allows you to issue CLI commands from within the browser window without opening a Telnet client. The functionality includes:

- SSH Support
- Command Completion
- Command History

To use the CLI Shell, you must first download and install a CLI proxy installable service/daemon. “CLIProxy_window” can be found on the Extreme Networks website (www.extremenetworks.com).

The figure below shows the **CLI Shell** screen of the ScreenPlay tool.

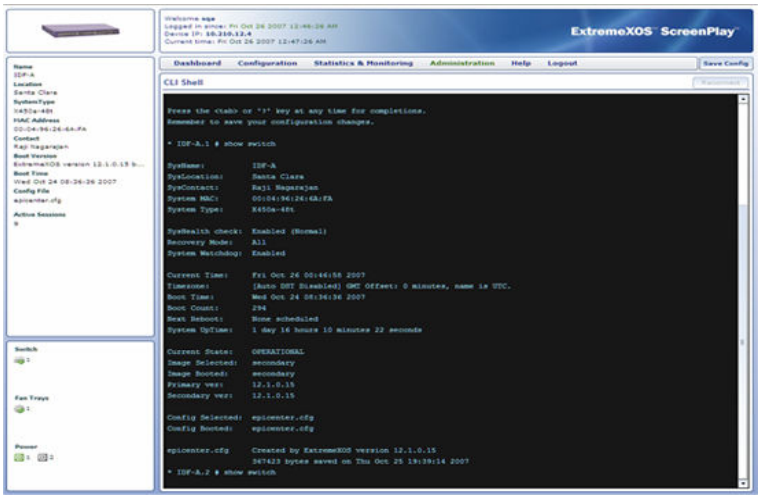


Figure 29: CLI Shell Screen

Screen/Pane	Description
CLI Shell	Displays a CLI screen on which commands can be entered. You can change the appearance of the screen. The settings for the foreground and background colors as well the CLI Shell Port can be reset.

7 Help

The Help menu includes the following functions:

- Services and Technical Support—opens the Services and Support page on Extreme Networks' website.
- *EXOS Command Reference Guide*—links to the current Command Reference Guide in PDF format.
- *EXOS Concepts Guide*—links to the current Cocepts Guide in PDF format.
- About—opens a standard information screen.